

7-3-00

A

06/30/00
JCS15 U.S. PTO
09/608735

COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, DC 20231

Attorney Docket: 1775P
PATENT

Transmitted herewith for filing is the Patent Application of:

Inventor(s): **Martin J. Pagel**

For: **EVIDENCING AND VERIFYING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY**

Enclosed with the Patent Application are:

- ☒ Six (6) sheets of Drawings
- ☒ Declaration and Power of Attorney
- ☒ Assignment and Recordation Form
- ☐ Information Disclosure Statement (PTO Form 1449)
- ☒ Small Entity Status Declaration
- ☒ Self Addressed, Stamped Postcard

JCS15 U.S. PTO
09/608735
06/30/00

The filing fee has been calculated as shown below:

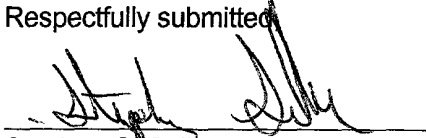
	(Col. 1)	(Col. 2)
FOR: NO. FILED		NO. EXTRA
BASIC FEE		
TOTAL CLAIMS		
35 - 20 =		15
INDEP. CLAIMS		
6 - 3 =		3
MULTIPLE DEPENDENT CLAIM PRESENTED		+250

SMALL ENTITY			
RATE		FEE	
		\$	345.00
x 9	=	\$	135.00
x 39	=	\$	117.00
	=	\$	0.00
TOTAL		\$	597.00

*If the difference in Col. 1 is less than "0", enter "0" in Col. 2

☒ Check No. 1710 in the amount of **\$ 597.00** is enclosed for payment of filing fees. The Commissioner is hereby authorized to charge any additional fees required or credit any overpayment to Deposit Account No. 02-2120.

SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, California 94303
(650) 493-4540

Respectfully submitted

Stephen G. Sullivan
Attorney for Applicants
Reg. No. 38,329

EXPRESS MAIL CERTIFICATE

I hereby certify that the above paper/fee is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on **June 30, 2000**, and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231. "Express Mail" no.: **EL547855213US**. Signature of Person mailing paper/fee:


Stephen G. Sullivan

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Pagel, M.

Serial No.

Filed: Herewith

For: **EVIDENCING AND VERIFYING INDICIA OF VALUE
USING SECRET KEY CRYPTOGRAPHY****DECLARATION CLAIMING SMALL ENTITY STATUS
UNDER 37 CFR 1.9(f) and 1.27(c) SMALL BUSINESS CONCERN**

I hereby declare that I am

- ☐ the owner of the small business concern identified below:
☒ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN

E-Stamp Corporation

ADDRESS OF CONCERN

2051 Stierlin Court
Mountain View, California 94043

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal years, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled **EVIDENCING AND VERIFYING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY** by inventor(s) Martin J. Pagel, described in application filed herewith.

The rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27).

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

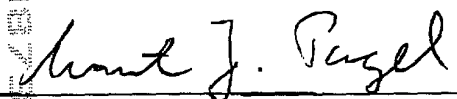
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this declaration is directed.

NAME OF PERSON SIGNING:

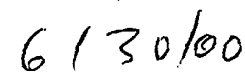
TITLE OF PERSON OTHER THAN OWNER:

ADDRESS OF PERSON SIGNING:

Martin J. Pagel**Chief Technical Officer****2051 Stierlin Court****Mountain View, California 94043**



Signature



Date

EVIDENCING AND VERIFYING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY

CROSS-REFERENCE TO RELATED APPLICATIONS

5 The present invention is related to co-pending U.S. Patent Application Serial No. ____
____ entitled "Evidencing Indicia of Value Using Secret Key Cryptography," which is
assigned to the assignee of the present application and filed on the same date as the present
application.

FIELD OF THE INVENTION

10 The present invention relates to Internet postage solutions, and more particularly to
evidencing and verifying any type of indicia indicating the value of goods or services using
secret key cryptography.

BACKGROUND OF THE INVENTION

15 Systems for allowing consumers to print postage indicia on mail, rather than
purchasing stamps from a post office, are well-known. An example of such a system is an
Internet postage system solution that was developed by the assignee of the present
application. As shown in FIG. 1, the system includes a United States Postal Service (USPS)
certificate authority 10, an operations center 12, a postage generating device 14 coupled
between a user's PC 16 and a printer 18, and multiple USPS distribution centers 20, which
also act as postage verifiers upon receipt of the mail.

20 A combination of software running on the user's PC 16 and the postage generating

device 14 enables the user to purchase postage from the operations center 12 via the Internet using a variety of payment options. Once obtained, the postage is secured and stored in the postage generating device 14. The user may then print a stamp in the form of a USPS-approved information based indicia (IBI) 22 onto envelopes, labels, or directly onto mail pieces while also printing the destination and return addresses. The IBI 22 is printed as a 2-D barcode that typically includes various information including the name of the user, the ID of the device, the amount of postage remaining, the zip code of the destination, and the date.

Since digital imaging, printing, photocopying, and scanning technology make it fairly easy to counterfeit the IBI 22, cryptographic methods, such as asymmetric public key cryptography, have been employed to generate and validate the IBI 22. In the prior art system shown in FIG. 1, for example, the certificate authority 10 transfers a digital certificate, which is a digitally signed public key, and a certificate ID to the postage generating device 14 via the operations center 12. When generating the IBI 22, the postage generating device 14 uses an internally generated private key and the public key to digitally sign the indicia, thereby creating a digital signature. The digital signature and the certificate ID are then included in the IBI 22.

After printing the stamp and applying it to the mail piece, the mail piece is dropped in a local mailbox. The local post office then transfers the mail to a local or originating distribution center 20a. The originating distribution center 20a scans the IBI 22 using a barcode scanner to read the information on the stamp including the certificate ID and the digital signature. The originating distribution center 20a uses the certificate ID to request from USPS authorization center 10 the same digital certificate used to sign the indicia in order to verify whether the IBI 22 is acceptable or fraudulent. All mail pieces with

acceptable IBI's 22 are then sorted by the first three digits of the zip code to determine the destination region. The sorted mail is then transferred from the origination distribution center 20a to the respective destination distribution center 20b located in the destination region. The destination distribution center 20b then finishes sorting the mail based on remaining digits of the zip code and the mail is delivered.

Many variations exist to the above scheme for evidencing and verifying postage. For example, US Patent 5,982,896 describes a symmetric fixed key set approach whereby instead of using a private key for each postage generating device 14, a set of keys is created where each key in the set is shared by multiple postage generating devices 14. In addition, the keys are made valid for only a limited amount of time to minimize the harm created by the theft of any of the keys and to limit the time for key attack.

Generating time-limited keys, however, requires that new keys be generated periodically and distributed to the postage generating devices 14. Because the step of distributing the keys typically occurs over the Internet or a private communications link, security for the keys becomes paramount. It is also important to ensure that only authorized devices use those keys.

The method described in Patent 5,982,896 for securing the keys has several disadvantages. One disadvantage is that the set of the shared keys used by the postage generating devices 14 are downloaded to the originating distribution centers 20 or other postage verifier. The shared keys are individually identified by pointers, which are also downloaded to the postage verifier, but are not cryptographically protected. Thus, the postage verifier has in its possession the entire set of cryptographic keys used by the postage generating devices 14. This fact makes the postage verifier a single point of attack: if the

verifier is broken into, a perpetrator may easily impersonate all postage generating devices
14 in the postal system.

Accordingly, what is needed is an improved method for evidencing and verifying
postage indicia. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The present invention provides a method and system for evidencing payment of
indicia using secret key cryptography. The method and system include a plurality of indicia
generating devices that are divided into groups for generating and printing indicia on a
media that is to be received at a plurality of establishments, wherein the establishments are
associated with different geographic designations. The method and system include assigning
a plurality of verification keys to each indicia generating device in each of the groups,
wherein each of the verification keys assigned to each of the groups is encrypted as a
function of a respective geographic designation. A key ID is associated with each of the
verification keys and is encrypted as a function of the same geographic designation used to
encrypt the corresponding verification key. After the verification keys and key ID's are
assigned, each one of the establishments receives the verification keys and the key ID's that
were encrypted as a function of the geographic designation associated with the
establishment. When generating indicia for media destined for a particular one of the
establishments, the indicia generating devices evidence the indicia by generating one of the
verification keys and the corresponding key ID assigned to indicia generating device's group
based on the geographic designation associated with the particular establishment, and uses
the generated verification key to create a digital signature. The indicia generating devices

digitally sign the indicia by including the digital signature and the generated key ID in the indicia. Upon receiving the media at the particular establishment, the indicia on the media is verified by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

In one embodiment, the method and system are used to generate and print indicia on media such as tickets, coupons, and the like that will be received by establishments, such as movie theatres and restaurants, for instance. In the preferred embodiment, however, the method and system are used to generate and print indicia for postage on mail that is to be received at a plurality of distribution centers. In this embodiment, the indicia printed on the mail is preferably verified at destination distribution centers, but may also be verified at an originating distribution centers.

According to the preferred embodiment of the method and system disclosed herein, postage validation is now performed at destination distribution centers, rather than at originating distribution centers, and the verification keys, which are encrypted as a function of the destination, are only distributed to the corresponding distribution centers. Thus, even if a destination center were broken into, the perpetrator would only be able to forge postal indicia for mail pieces destined for the particular destination. In addition, the key ID is also encrypted so that even if a perpetrator were to crack a verification key, the perpetrator would still have a problem identifying which verification key was obtained. In order to forge the indicia, the perpetrator must possess two keys, rather than one, a secret key that the PGD used to compute the key ID, and the verification key itself.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a prior art Internet postage system.

FIG. 2 is a block diagram illustrating a postage evidencing and verification system in accordance with a preferred embodiment of the present invention.

FIG. 3 is a flow chart illustrating the process of evidencing payment of postage using secret key cryptography in the evidencing and verification system of the present invention.

FIG. 4 is a flow chart illustrating in detail the process the KDC uses to generate and distribute cryptographic keys for postage evidencing and verification in accordance with the present invention.

FIG. 5 is a flow chart illustrating the process of dispensing and evidencing postage indicia within the postage generating devices in accordance with a preferred embodiment of the present invention.

FIG. 6 is a flow chart illustrating the process of verifying postage indicia at a plurality of postal distribution centers in accordance with the present invention.

DETAILED DESCRIPTION

The present invention relates to using key cryptography for evidencing and verifying postage. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment and the generic principles and features described herein will be readily apparent to those skilled in the art. Thus, the present invention is not intended to be limited to the embodiments shown but is to be accorded the widest scope consistent with the principles and features described herein.

FIG. 2 is a block diagram illustrating a postage evidencing and verification system in accordance with a preferred embodiment of the present invention, where like components from FIG. 1 have like reference numerals. In a preferred embodiment, the system includes a key distribution center 24, a plurality of postage generating devices (PGDs) 14, and multiple USPS distribution centers 20. The PGDs 14 may be implemented as a computing device separate from the PC 16 (FIG. 1), as software running on the PC 16, or any processing device, such as a cellphone or PDA, or any combination of the two. The function of the key distribution center 24 is to provide the cryptographic keys used by the PGDs 14 to evidence postage, and used by the distribution centers 20 to verify the postage. In a preferred embodiment, the key distribution center 24 distributes the cryptographic keys to the PGDs 14 and to the distribution centers 20 via a telecommunications network, such as the Internet or private link, although other types of distribution methods may also be used. In a preferred embodiment, the key distribution center (KDC) 24 authenticates and distributes the keys via asymmetric encryption to ensure the privacy of the keys and that only authorized devices receive the keys. The KDC 24 may be the USPS certificate authority, or other third party service.

FIG. 3 is a flow chart illustrating the process of evidencing payment of postage using secret key cryptography in the evidencing and verification system of the present invention. Referring to both FIGS. 2 and 3, the process begins by the KDC 24 dividing the PDG's into n groups 26, G_i , $i = 1, \dots, n$, in step 28. The KDC 24 then in step 30 assigns a set of verification keys 21, V_i , to each PGD group 26, where each verification key in the set is encrypted as a function of one of the destination regions. In a preferred embodiment, each destination region corresponds to a zip code region, so the number of verification keys

assigned to each PDG group 26 depends on the number of existing zip code regions (shown in Fig. 2 as Dest1...Destx).

The KDC 24 also assigns in step 32 a set of key ID's 23, I_i , to each PDG group 26, where each key ID in the set is associated with one of the assigned verification keys and is encrypted as a function of the same destination region used to encrypt the corresponding verification key. Referring to Fig. 2, the result of steps 30 and 32 is that the column of verification keys 21 and key ID's 23 $\{V_i$ and $I_i\}$ are assigned to PDG group G_1 , the column of verification keys and key ID's $\{V_i$ and $G_i\}$ are assigned to PDG group G_i , and so on.

Referring again to FIG. 3, in a preferred embodiment, it is also required that postal verification of the postage indicia be performed at the plurality of destinations regions, rather than the originating region, in step 34. The postage verification may be performed at the destination distribution centers 20b or by a third party verifier that is in remote communication with the KDC 24.

After assigning the verification keys 21 to the PGD groups 26, the KDC 24 distributes to each distribution center the sets of verification keys 21 and key ID's 23 that were encrypted as a function of the corresponding destination region in step 36. Thus, in Fig. 2 for example, all the verification keys 21 and key ID's 23, V^{Dest1} and I^{Dest1} , respectively, would only be distributed to the Distribution center in the destination region designated as "Dest1".

According to another aspect of the present invention, when generating the postage indicia for a mail piece destined for a particular destination, in step 38 the PGD 14 generates one of the verification keys and its corresponding key ID from the set of keys assigned to its group based on the particular destination. By requiring the PGD 14 to generate the

verification key, rather than distributing the verification key to the PGD 14, a perpetrator cannot infiltrate the PGD 14 and copy the verification key. The PGD 14 then uses the generated verification key to create a digital signature for the indicia using any well-known message authentication code (MAC) function, and digitally signs the indicia by including the digital signature and the generated key ID on the indicia in step 40.

When the mail is received at the destination region, the indicia is verified using the key ID from the indicia, and the verification keys received from the KDC 24, to compute a new digital signature for the indicia, and by comparing the computed digital signature with the digital signature on the indicia in step 42.

FIG. 4 is a flow chart illustrating in more detail the process the KDC 24 uses to generate and distribute cryptographic keys for postage evidencing and verification in accordance with the present invention. The KDC 24 begins by creating a master secret key 25, K , and a set of secret keys 27, and assigns each secret key, K_i , to one of the PDG groups, G_i , in step 52.

The KDC 24 in step 54 also generates and assigns a set of n verification keys, V_i^{Dest} , $i = 1, \dots, n$, for each PGD group G_i , where each of the verification keys is calculated as a function of a respective destination region. In a preferred embodiment, each postage verification key V_i^{Dest} is computed as a one-way function of the PGD group secret key K_i and the designation of the postal destination:

$$V_i^{Dest} = H(K_i, Dest)$$

where H may be a one-way function such as md5 (Message Digest 5) or sha-1

(Secure Hash Algorithm-1), and *Dest* is a designation of the destination region, which in a preferred embodiment, is the first three digits of the destination ZIP code or a first few characters of the postal code.

After generating the verification keys, the KDC 24 in step 56 generates and assigns a set of key ID's, I_i^{Dest} , $i = 1, \dots, n$, for each group, where each key ID corresponds to one of the verification keys assigned to that group and is also generated as a function of a respective destination region. In a preferred embodiment, each key ID is computed as a one-way hash function of the PGD group, G_i , the master secret key, K , and a designation of the destination, *Dest*:

$$I_i^{Dest} = H(K, Dest, G_i)$$

It should be noted that the size of the key ID is selected such that there are no collisions among the key IDs for a particular destination designation.

According to one aspect of the present invention, the keys are distributed in such a manner that each PGD 14 is made unaware of which group verification key V it will use to evidence postage indicia. This is accomplished by transferring only the master secret key K and the group secret key K_i to all PGD's 14 in group G_i in step 58. In addition, only the verification keys V_i^{Dest} and Key ID's I_i^{Dest} generated as a function of a particular destination region are transferred to the corresponding distribution center in step 60, rather than transferring all of the groups of verification keys to all destination distribution centers. In a preferred embodiment, the verification keys V_i^{Dest} and indexes I_i^{Dest} are stored in secure tables at the distribution centers 20.

After all keys have been distributed, the PGDs 14 may perform the process of

dispensing and evidencing postage indicia.

FIG. 5 is a flow chart illustrating the process of dispensing and evidencing postage indicia within the postage generating devices 14 in accordance with a preferred embodiment of the present invention. The process begins in step 70 by receiving a master secret key K and a secret key K_i from the KDC 24. In response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination $Dest$, the indicium is generated in step 72, and the verification key V_i^{Dest} is computed in step 74 as a function of the secret key K_i and the destination. In a preferred embodiment, the PGD 14 computes the verification key V_i^{Dest} using the function H :

$$V_i^{Dest} = H(K_i, Dest)$$

The PGD 14 also computes the encrypted key ID I_i^{Dest} as a function of the destination in step 76. In a preferred embodiment, the PGD 14 computes the key ID I_i^{Dest} using its assigned group designation G_i , the master secret key K shared between all postage-generating devices, and the designation of the postal destination $Dest$:

$$I_i^{Dest} = H(K, Dest, G_i)$$

The PGD 14 evidences the indicia in step 78 by creating a digital signature for the indicia using the verification key V_i^{Dest} and digitally signs the indicia by including the digital signature and the computed index I_i^{Dest} on the indicia. The mail piece bearing the postage indicia is now ready for mailing and subsequent verification.

FIG. 6 is a flow chart illustrating the process of verifying postage indicia at a plurality of postal distribution centers in accordance with the present invention. First, in step

90 each of the destination distribution centers 20 receives from the KDC 24 a set of verification keys V_i^{Dest} and the key ID's I_i^{Dest} that were generated as a function of the destination region the distribution center 20 services. In a preferred embodiment, the keys are delivered over the Internet and stored in a secure table.

5 In response to receiving a mail piece, each of the distribution centers 20 determines the mail piece's destination region in step 92. If the distribution center is not within the destination region, then the distribution transfers the mail piece to the destination distribution center 20b within the destination region in step 94.

If the distribution center is within the destination region, then the distribution center begins verifying the postage indicia by reading the digital signature and the key ID from the indicia in step 96. The key ID read from the indicia is then used to retrieve the corresponding verification key that was used to create the digital signature from the table containing the verification keys in step 98. The retrieved verification key is then used to compute a new digital signature from the indicia, and the computed digital signature is then compared with the digital signature from the indicia to verify the indicia in step 100.

15 In accordance with a second embodiment of the present invention, the verification keys and the key ID's are computed as a function of the originating distribution region, rather than the destination region. In this embodiment, the each distribution center 20 still receives the verification keys computed as a function of the region the distribution center services, but the PDGs 14 compute their verification keys based on the originating region where they are located (e.g., the zip code of the return address), and verification of the postage indicia is performed at the originating distribution center where the mail is deposited.

09606735 "063000
5522990
5
10
15

In accordance with a third embodiment of the present invention, the evidencing and verification system may also be used for issuing and evidencing any indicia indicating the value of goods and/or services, such as tickets, coupons, and gift certificates, for instance. In one embodiment, an indicia generating device generates and prints indicia on a media that is to be received at various predetermined destinations. For example, the key distribution center 24 may provide cryptographic keys to a chain of movie theaters, for instance. In this system, the key distribution could service the movie theater chain and issue separate keys for different venues. The operator of each local movie theater could download new keys from the key distribution center 24 periodically (e.g., everyday). In turn, moviegoers having access to a PGD 14 would then download the master secret key and the secret key for their device group from the local movie theater via the Internet. After receiving the keys, the PGD 14 would print and evidence movie tickets, and each movie theater would perform the verification function for verifying the tickets.

Thus, the present invention is applicable to generating and evidencing indicia of value for any media that is to be received at establishments associated with geographic designations, such as addresses and zip codes.

20
The indicia evidencing and verification system in accordance with the present invention offers significant advantages over prior methods for verifying cryptographic postage evidencing. One advantage is that the verification center is no longer a single point of failure in the postal system, since the verification center does not contain all the verification keys. Because the present invention performs verification only at destination distribution centers 20b and encrypts the keys as a function of the destination, even if a destination center 20b were broken into, the perpetrator would only be able to forge postal

indicia for mail pieces destined for the particular destination. Security is not as tight in the second preferred embodiment, however, where the keys are encrypted as a function of the origin and verification is performed at the originating distribution centers 20a, because if an originating distribution center 20a were broken into, the perpetrator would be able to forge postal indicia for all mail pieces as long as every mail piece was mailed from that particular originating distribution center 20a .

Another advantage is that since the PGD 14 encrypts the key ID and sends the key ID along with the verification key on the postage indicia, even if a perpetrator were to crack a verification key, the perpetrator would still have a problem identifying which verification key was obtained. In order to forge the indicia, the perpetrator must possess the secret key that the PGD 14 used to compute the key ID, and the verification key itself. This means that the perpetrator must possess two secret keys rather one in order to forge the postage indicia.

The present invention has been described in accordance with the embodiments shown, and one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and any variations would be within the spirit and scope of the present invention.

In addition, software written according to the present invention may be stored on a computer-readable media, such as a removable memory, or transmitted over a network, and loaded into the key distribution center computers, the user's PC, the PGD, and distribution center computers for execution. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

CLAIMS

What is claimed is:

- 1 1 A method for evidencing payment of indicia using secret key cryptography in a system
2 including a plurality of indicia generating devices that are divided into groups, each of the
3 indicia generating devices for generating and printing indicia on a media that is to be
4 received at a plurality of establishments, wherein the establishments are associated with
5 different geographic designations, the method comprising the steps of:
- 6 (a) assigning a plurality of verification keys to each indicia generating device in
7 each of the groups, wherein each of the verification keys assigned to each of
8 the groups is encrypted as a function of a respective geographic designation;
 - 9 (b) associating a key ID with each of the verification keys and encrypting each
10 key ID as a function of the same geographic designation used to encrypt the
11 corresponding verification key;
 - 12 (c) distributing to each one of the establishments, the verification keys and the
13 key ID's that were encrypted as a function of the geographic designation
14 associated with the establishment;
 - 15 (d) using one of the indicia generating devices to generate indicia for media
16 destined for a particular one of the establishments, and evidencing the indicia
17 by
 - 18 (i) generating one of the verification keys and the corresponding key ID

assigned to indicia generating device's group based on the
geographic designation associated with the particular establishment,
and

(ii) using the generated verification key to create a digital signature, and
digitally signing the indicia by including the digital signature and the
generated key ID in the indicia; and

(e) upon receiving the media at the particular establishment, verifying the indicia
on the media using the key ID on the indicia and the distributed verifications
keys to compute a digital signature, and comparing the computed digital
signature with the digital signature on the indicia.

2 The method of claim 1 further including the steps of:

assigning a secret key to each of the groups, and

encrypting the verification keys assigned to each group as a function of the secret key
and the different geographic designations.

3 The method of claim 2 further including the steps of:

generating a master key; and

encrypting the key ID as a function of the master key, the geographic designation,
and a designation of the group.

4 The method of claim 3 further including the step of generating and printing indicia for
postage on a mail piece that is to be received at a plurality of distribution centers.

1
1 5 The method of claim 4 further including the step of verifying the indicia at a destination
2 distribution center.

1
1 6 The method of claim 4 further including the step of verifying the indicia at an originating
2 distribution center.

1
1 7 The method of claim 3 further including the step of using zip codes to represent the
2 geographic designations.

1
1 8 The method of claim 1 further including the step of generating and printing indicia for
2 tickets.

1
1 9 A method for evidencing payment of postage using secret key cryptography in a system
2 including a plurality of postage generating devices that are divided into groups, each of the
3 postage generating devices for generating postage indicia for mail destined for
4 predetermined postal destinations, the method comprising the steps of:

5 (a) assigning a plurality of verification keys to each indicia generating device in
6 each of the groups, wherein each of the verification keys assigned to each of
7 the groups is encrypted as a function of a respective ;

8 (b) associating a key ID with each of the verification keys and encrypting each
9 key ID as a function of the same destination used to encrypt the

10 corresponding verification key;

11 (c) requiring that verifiers of the postage indicia perform postal verification at the
12 plurality of destinations, where each verifier services a respective destination;

13 (d) distributing to each respective destination verifier, the verification keys and
14 the key ID's that were encrypted as a function of the corresponding
15 destination; and

16 (e) requiring each of the postage generating devices to evidence the postage
17 indicia for a mail piece destined for a particular destination by

18 (i) generating one of the verification keys and the corresponding key ID
19 assigned to its group based on that particular destination, and

20 (ii) using the generated verification key to create a digital signature, and
21 digitally signing the indicia by including the digital signature and the
22 generated key ID on the indicia, such that when the mail is received at
23 the predetermined destination, the verifier uses the key ID on the
24 indicia and the distributed verifications keys to compute a digital
25 signature, and compares the computed digital signature with the
26 digital signature on the postage indicia to verify the postage indicia.

1
1 10 The method of claim 9 further including the steps of:

2 assigning a secret key to each of the groups, and

3 encrypting the verification keys assigned to each group as a function of the secret key
4 and the plurality of destinations.

1 11 The method of claim 10 further including the steps of:

2 generating a master key; and

3 encrypting the key ID as a function of the master key, the destination, and a
4 designation of the group.

1
1 12 The method of claim 11 further including the step of performing postage verification
2 onsite at a destination distribution center.

1
1 13 The method of claim 12 further including the step of performing postage verification by
2 a third party that is in remote communication with the destination distribution center.

1
1 14 The method as in claim 13 wherein the verifier further performs the steps of using the
2 key ID to retrieve the corresponding verification key used to originally create the digital
3 signature.

1
1 15 A system for evidencing payment of postage using secret key cryptography, comprising:
2 a plurality of postage generating devices that are divided into groups, each of the
3 postage generating devices for generating postage indicia for mail destined
4 for predetermined postal destinations;
5 a plurality of distribution centers for verifying the postage indicia, where each
6 distribution center services at least one of the postage destinations; and
7 a key distribution center in communication with the plurality of postage generating

8 devices and with the plurality of distribution centers, the key distribution
9 center for performing the functions of:

10 assigning a plurality of verification keys to each indicia generating
11 device in each of the groups, wherein each of the verification
12 keys assigned to each of the groups is encrypted as a function
13 of a respective destination, and for associating a key ID with
14 each of the verification keys and encrypting each key ID as a
15 function of the same destination used to encrypt the
16 corresponding verification key, and

17 distributing to each of the plurality of distribution centers, the
18 verification keys and the key ID's encrypted as a function of
19 the destination the distribution center services,

20 wherein in response to a request to generate indicia for a mail piece destined for a
21 particular destination, each of the postage generating devices generates one of
22 the verification keys and the corresponding key ID assigned to its group
23 based on that particular destination, and uses the generated verification key to
24 create a digital signature for the indicia, such that when the mail is received at
25 the distribution center servicing the predetermined destination, the key ID
26 from the indicia and the verification keys distributed to the distribution center
27 are used to verify the digital signature on the postage indicia.

1
1 16 The system of claim 15 wherein the key distribution center further generates a master
2 key, and a secret key for each of the postage generating devices groups, and distributes the

3 master key and the secret key to the respective postage generating devices within each of the
4 groups.

1
1 17 The system of claim 16 wherein the verification keys assigned to each group are
2 encrypted as a function of the secret key and the plurality of destinations.

1
1 18 The system of claim 17 further wherein the key ID is encrypted as a function of the
2 master key, the destination, and a designation of the group.

1
1 19 The system of claim 18 wherein verification of the postage is performed onsite at the
2 destination distribution centers.

1
1 20 The system of claim 19 wherein verification of the postage is performed by a third party
2 that is in remote communication with the destination distribution centers.

1
1 21 The system as in claim 20 wherein the indicia is verified by using the key ID from the
2 indicia to retrieve the corresponding verification key used to originally create the digital
3 signature, wherein the retrieved verification key is used to compute the digital signature for
4 the indicia and the computed digital signature is compared with the digital signature from
5 the indicia.

1
1 22 A computer-readable media containing program instructions for evidencing payment of
2 postage using secret key cryptography in a system including a plurality of postage

3 generating devices that are divided into groups, each of the postage generating devices for
4 generating postage indicia for mail destined for predetermined postal destinations from
5 among a plurality of destinations, the program instructions for:

- 6 (a) assigning a plurality of verification keys to each indicia generating device in
7 each of the groups, wherein each of the verification keys assigned to each of
8 the groups is encrypted as a function of a respective destination;
- 9 (b) associating a key ID with each of the verification keys and encrypting each
10 key ID as a function of the same destination used to encrypt the
11 corresponding verification key;
- 12 (c) requiring that verifiers of the postage indicia perform postal verification at the
13 plurality of destinations, where each verifier services a respective destination;
- 14 (d) distributing to each respective destination verifier, the verification keys and
15 the key ID's that were encrypted as a function of the corresponding
16 destination; and
- 17 (e) requiring each of the postage generating devices to evidence the postage
18 indicia for a mail piece destined for a particular destination by
 - 19 (i) generating one of the verification keys and the corresponding key ID
20 assigned to its group based on that particular destination, and
 - 21 (ii) using the generated verification key to create a digital signature, and
22 digitally signing the indicia by including the digital signature and the
23 generated key ID on the indicia, such that when the mail is received at
24 the predetermined destination, the verifier uses the key ID on the
25 indicia and the distributed verifications keys to compute a digital

signature, and compares the computed digital signature with the digital signature on the postage indicia to verify the postage indicia.

23 The computer-readable media of claim 22 further including the instructions of:

assigning a secret key to each of the groups, and

encrypting the verification keys assigned to each group as a function of the secret key and the plurality of destinations.

24 The computer-readable media of claim 23 further including the instructions of:

generating a master key; and

encrypting the key ID as a function of the master key, the destination, and a designation of the group.

25 The computer-readable media of claim 24 further including the instruction of performing postage verification onsite at a destination distribution center.

26 The computer-readable media of claim 25 further including the instruction of performing postage verification by a third party that is in remote communication with the destination distribution center.

27 The computer-readable media as in claim 26 further including the instructions of using the key ID to retrieve the corresponding verification key used to originally create the digital signature.

1
1 28 A method for generating and distributing cryptographic keys for postage evidencing and
2 verification in a system where mail is destined for predetermined postal destinations ,
3 wherein each of the postal destinations is serviced by a postal distribution center, the method
4 comprising the steps of:

- 5 (a) creating a master secret key K ;
- 6 (b) dividing a plurality of postage generating devices (PGDs) that generate
7 postage indicia for mail into n groups $G_i, i = 1, \dots, n$;
- 8 (c) assigning each PDG group, G_i , a secret key K_i ;
- 9 (d) generating a set of n verification keys, $V_i^{Dest}, i = 1, \dots, n$, for each PGD group
10 G_i , where each of the verification keys is calculated as a function of a
11 respective postal destination (Dest);
- 12 (e) generating a set of key ID's, $I_i^{Dest}, i = 1, \dots, n$, where each key ID corresponds
13 to one of the verification keys and is also generated as a function the same
14 postal destination used to calculate the corresponding verification key;
- 15 (f) transferring to each distribution center, the verification keys V_i^{Dest} and key
16 ID's I_i^{Dest} that were calculated as a function of the destination serviced by
17 the distribution center; and
- 18 (g) transferring the master secret key K and the secret key K_i to all PGD's in
19 group G_i , such that each PGD, when evidencing indicia for the mail destined
20 for one of the predetermined postal destination, generates one of the
21 verification keys based on the predetermined postal destination to create a

digital signature for the indicia.

The method of claim 28 further including the step of computing each verification key V_i^{Dest} as a one-way function H of the PGD group key K_i and a designation of the postal destination:

$$V_i^{Dest} = H(K_i, Dest).$$

The method of claim 29 further including the step of using ZIP codes to designate the plurality of postal destinations.

The method of claim 30 further including the step of computing each of the key ID's as a one-way function H of the PGD group, G_i , the master secret key, K , and a designation of the postal destination, $Dest$:

$$I_i^{Dest} = H(K, Dest, G_i).$$

A method for verifying postage indicia a mail piece received at a postal distribution center that services a particular postal region, comprising the steps of:

- (a) receiving and storing a set of verification keys V_i^{Dest} and a set of key ID's I_i^{Dest} identifying the verification keys, wherein the verification keys and the key ID's were generated as a function of the postal region;
- (b) in response to receiving the mail piece, determining the mail piece's postal region;

- 8 (c) if the distribution center is not within the mail piece's destination region,
9 transferring the mail piece to the distribution center within the mail piece's
10 postal region; and
- 11 (d) if the distribution center is within the mail piece's postal region, verifying the
12 postage indicia by
- 13 (i) reading a digital signature and a key ID from the indicia,
 - 14 (ii) using the key ID read from the indicia to retrieve the corresponding
15 verification key from the stored set of verification keys,
 - 16 (iii) using the retrieved verification key to compute a digital signature for
17 the indicia, and
 - 18 (iv) comparing the computed digital signature with the digital signature
19 read from the postage indicia to verify the indicia.

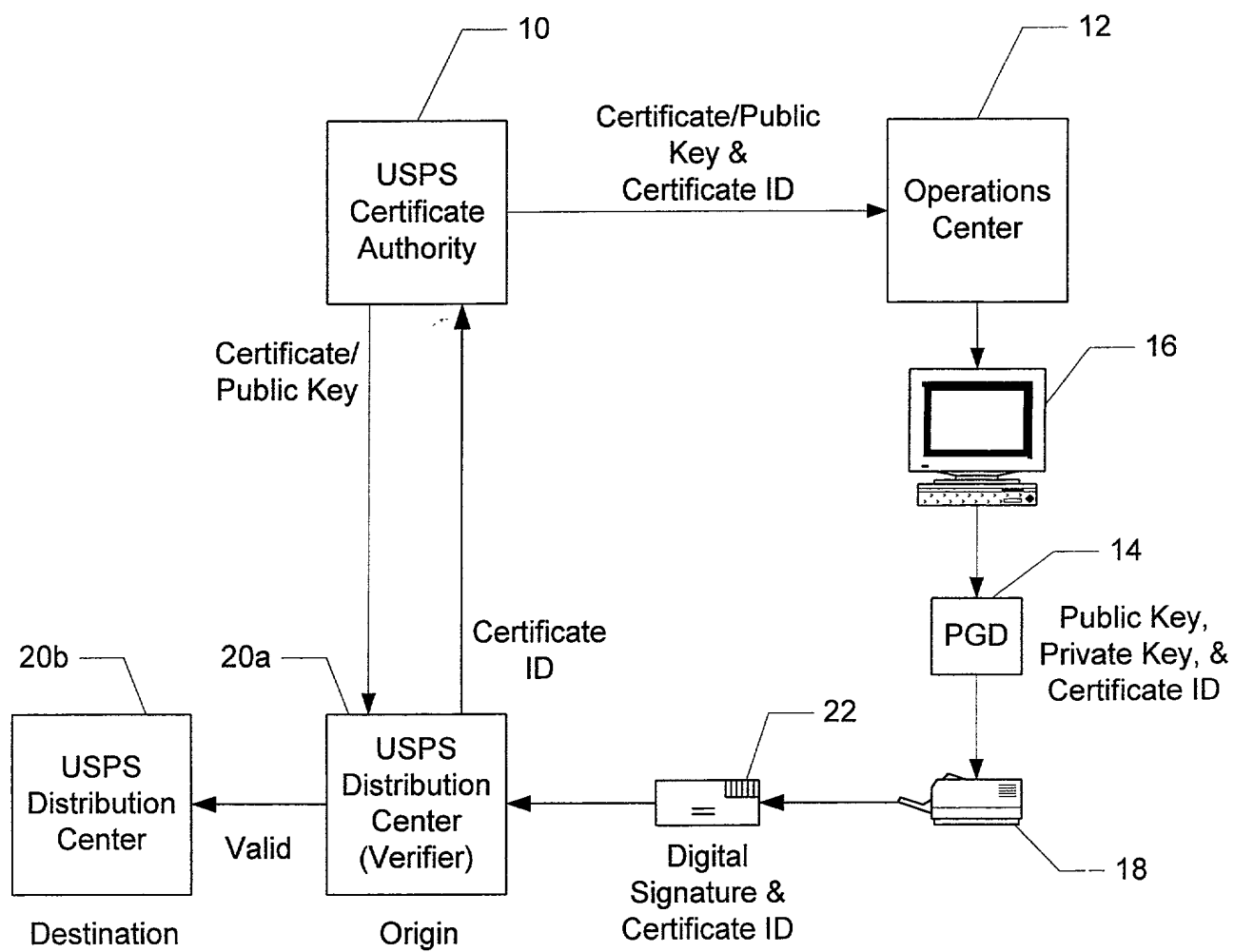
20
21
22
23
24
25
26
27
28
29
30
31
32
33 The method of claim 32 further including the step of determining the mail piece's postal
34 region based on a zip code.

35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
220

ABSTRACT

A method and system for evidencing payment of indicia using secret key cryptography is disclosed. The method and system include a plurality of indicia generating devices that are divided into groups for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations. The method and system include assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective geographic designation. A key ID is associated with each of the verification keys and is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key. After the verification keys and key ID's are assigned, each one of the establishments receives the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment. When generating indicia for media destined for a particular one of the establishments, the indicia generating devices evidence the indicia by generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and uses the generated verification key to create a digital signature. The indicia generating devices digitally sign the indicia by including the digital signature and the generated key ID in the indicia. Upon receiving the media at the particular establishment, the indicia on the media is verified by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.

Table 1. The continued	
1990	100
1991	100
1992	100
1993	100
1994	100
1995	100
1996	100
1997	100
1998	100
1999	100
2000	100
2001	100
2002	100
2003	100
2004	100
2005	100
2006	100
2007	100
2008	100
2009	100
2010	100
2011	100
2012	100
2013	100
2014	100
2015	100
2016	100
2017	100
2018	100
2019	100
2020	100
2021	100
2022	100
2023	100
2024	100
2025	100
2026	100
2027	100
2028	100
2029	100
2030	100
2031	100
2032	100
2033	100
2034	100
2035	100
2036	100
2037	100
2038	100
2039	100
2040	100
2041	100
2042	100
2043	100
2044	100
2045	100
2046	100
2047	100
2048	100
2049	100
2050	100
2051	100
2052	100
2053	100
2054	100
2055	100
2056	100
2057	100
2058	100
2059	100
2060	100
2061	100
2062	100
2063	100
2064	100
2065	100
2066	100
2067	100
2068	100
2069	100
2070	100
2071	100
2072	100
2073	100
2074	100
2075	100
2076	100
2077	100
2078	100
2079	100
2080	100
2081	100
2082	100
2083	100
2084	100
2085	100
2086	100
2087	100
2088	100
2089	100
2090	100
2091	100
2092	100
2093	100
2094	100
2095	100
2096	100
2097	100
2098	100
2099	100
2100	100
2101	100
2102	100
2103	100
2104	100
2105	100
2106	100
2107	100
2108	100
2109	100
2110	100
2111	100
2112	100
2113	100
2114	100
2115	100
2116	100
2117	100
2118	100
2119	100
2120	100
2121	100
2122	100
2123	100
2124	100
2125	100
2126	100
2127	100
2128	100
2129	100
2130	100
2131	100
2132	100
2133	100
2134	100
2135	100
2136	100
2137	100
2138	100
2139	100
2140	100
2141	100
2142	100
2143	100
2144	100
2145	100



PRIOR ART

FIG. 1

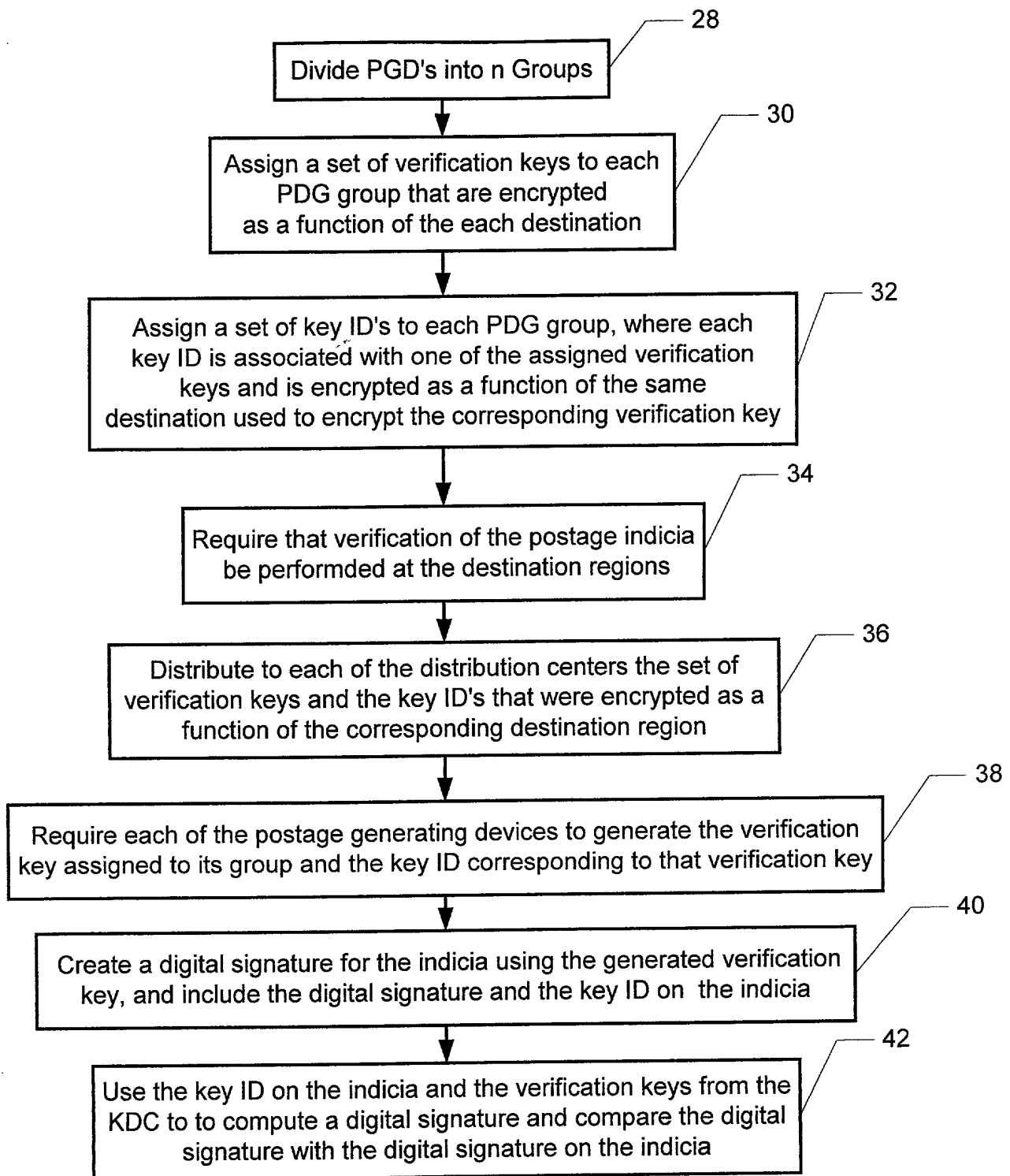


FIG. 3

```
graph TD; 52[Create a master secret key, K, and set of secret keys, and assign each secret key, Ki, to a group of PGD's, Gi] --> 54[Generate and assign a set of n verification keys, Vi, for each PGD group Gi, where each of the verification keys is calculated as a function of a respective destination region]; 54 --> 56[Generate and assign a set of key ID's, Ii^Dest, for each PGD group, where each key ID identifies one of the verification keys assigned to that group and is also generated as a function a respective destination region]; 56 --> 58[Transfer only the master secret key K and the secret key Ki to all PGD's in group Gi]; 58 --> 60[Transfer only the verification keys and the key ID's that were generated as a function of a particular destination to the corresponding destination distribution center];
```

52 Create a master secret key, K, and set of secret keys, and assign each secret key, K_i , to a group of PGD's, G_i

54 Generate and assign a set of n verification keys, V_i , for each PGD group G_i , where each of the verification keys is calculated as a function of a respective destination region

56 Generate and assign a set of key ID's, I_i^{Dest} , for each PGD group, where each key ID identifies one of the verification keys assigned to that group and is also generated as a function a respective destination region

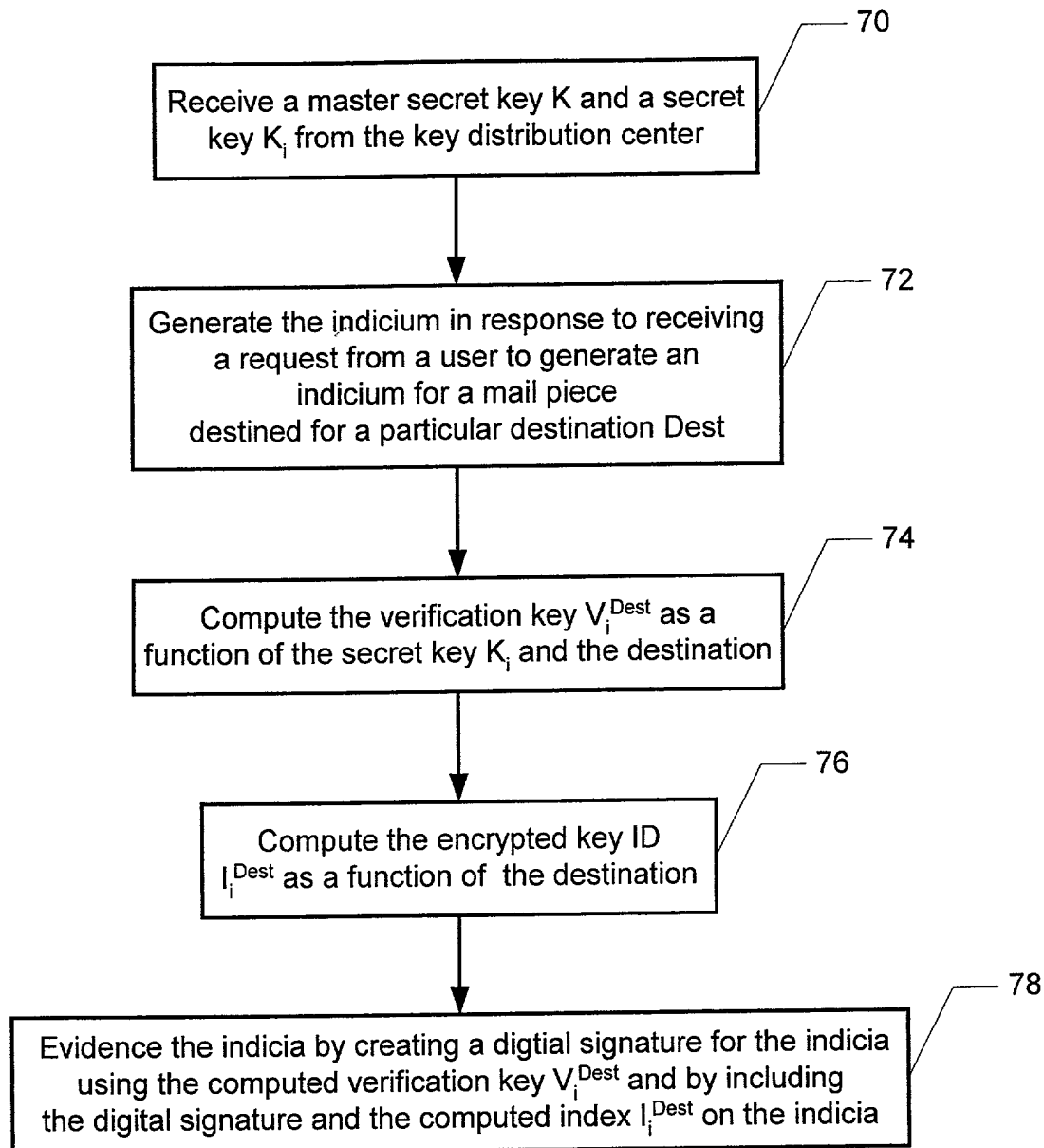
58 Transfer only the master secret key K and the secret key K_i to all PGD's in group G_i

60 Transfer only the verification keys and the key ID's that were generated as a function of a particular destination to the corresponding destination distribution center

Generation and Distribution of Keys

FIG. 4

Bacterial strains	
Strain	Source
ATCC 25922	ATCC
ATCC 43269	ATCC
ATCC 49224	ATCC
ATCC 50068	ATCC
ATCC 50070	ATCC
ATCC 50071	ATCC
ATCC 50072	ATCC
ATCC 50073	ATCC
ATCC 50074	ATCC
ATCC 50075	ATCC
ATCC 50076	ATCC
ATCC 50077	ATCC
ATCC 50078	ATCC
ATCC 50079	ATCC
ATCC 50080	ATCC
ATCC 50081	ATCC
ATCC 50082	ATCC
ATCC 50083	ATCC
ATCC 50084	ATCC
ATCC 50085	ATCC
ATCC 50086	ATCC
ATCC 50087	ATCC
ATCC 50088	ATCC
ATCC 50089	ATCC
ATCC 50090	ATCC
ATCC 50091	ATCC
ATCC 50092	ATCC
ATCC 50093	ATCC
ATCC 50094	ATCC
ATCC 50095	ATCC
ATCC 50096	ATCC
ATCC 50097	ATCC
ATCC 50098	ATCC
ATCC 50099	ATCC
ATCC 50100	ATCC
ATCC 50101	ATCC
ATCC 50102	ATCC
ATCC 50103	ATCC
ATCC 50104	ATCC
ATCC 50105	ATCC
ATCC 50106	ATCC
ATCC 50107	ATCC
ATCC 50108	ATCC
ATCC 50109	ATCC
ATCC 50110	ATCC
ATCC 50111	ATCC
ATCC 50112	ATCC
ATCC 50113	ATCC
ATCC 50114	ATCC
ATCC 50115	ATCC
ATCC 50116	ATCC
ATCC 50117	ATCC
ATCC 50118	ATCC
ATCC 50119	ATCC
ATCC 50120	ATCC
ATCC 50121	ATCC
ATCC 50122	ATCC
ATCC 50123	ATCC
ATCC 50124	ATCC
ATCC 50125	ATCC
ATCC 50126	ATCC
ATCC 50127	ATCC
ATCC 50128	ATCC
ATCC 50129	ATCC
ATCC 50130	ATCC
ATCC 50131	ATCC
ATCC 50132	ATCC
ATCC 50133	ATCC
ATCC 50134	ATCC
ATCC 50135	ATCC
ATCC 50136	ATCC
ATCC 50137	ATCC
ATCC 50138	ATCC
ATCC 50139	ATCC
ATCC 50140	ATCC
ATCC 50141	ATCC
ATCC 50142	ATCC
ATCC 50143	ATCC
ATCC 50144	ATCC
ATCC 50145	ATCC
ATCC 50146	ATCC
ATCC 50147	ATCC
ATCC 50148	ATCC
ATCC 50149	ATCC
ATCC 50150	ATCC
ATCC 50151	ATCC
ATCC 50152	ATCC
ATCC 50153	ATCC
ATCC 50154	ATCC
ATCC 50155	ATCC
ATCC 50156	ATCC
ATCC 50157	ATCC
ATCC 50158	ATCC
ATCC 50159	ATCC
ATCC 50160	ATCC
ATCC 50161	ATCC
ATCC 50162	ATCC
ATCC 50163	ATCC
ATCC 50164	ATCC
ATCC 50165	ATCC
ATCC 50166	ATCC
ATCC 50167	ATCC
ATCC 50168	ATCC
ATCC 50169	ATCC
ATCC 50170	ATCC
ATCC 50171	ATCC
ATCC 50172	ATCC
ATCC 50173	ATCC
ATCC 50174	ATCC
ATCC 50175	ATCC
ATCC 50176	ATCC
ATCC 50177	ATCC
ATCC 50178	ATCC
ATCC 50179	ATCC
ATCC 50180	ATCC
ATCC 50181	ATCC
ATCC 50182	ATCC
ATCC 50183	ATCC
ATCC 50184	ATCC
ATCC 50185	ATCC
ATCC 50186	ATCC
ATCC 50187	ATCC
ATCC 50188	ATCC
ATCC 50189	ATCC
ATCC 50190	ATCC
ATCC 50191	ATCC
ATCC 50192	ATCC
ATCC 50193	ATCC
ATCC 50194	ATCC
ATCC 50195	ATCC
ATCC 50196	ATCC
ATCC 50197	ATCC
ATCC 50198	ATCC
ATCC 50199	ATCC
ATCC 50200	ATCC
ATCC 50201	ATCC
ATCC 50202	ATCC
ATCC 50203	ATCC
ATCC 50204	ATCC
ATCC	



Dispensing & Evidencing Postage Indicia

FIG. 5

```
graph TD; 90[Receive the verification keys  $V_i^{Dest}$  and key ID's  $I_i^{Dest}$  generated as a function of the destination region serviced by the distribution center] --> 92[In response to receiving a mail piece, determine the mail piece's destination region]; 92 --> 94[If the distribution center is not within the destination region, transfer the mail piece to the distribution center within the destination region]; 94 --> 96[If the distribution center is within the destination region, begin verifying the postage indicia by reading the digital signature and the key ID from the indicia]; 96 --> 98[Use the key ID read from the indicia to retrieve the corresponding verification key from the table of all verification keys]; 98 --> 100[Use the retrieved verification key to compute a digital signature for the indicia, and compare the computed digital signature with the digital signature from the postage indicia to verify the indicia];
```

100

90 Receive the verification keys V_i^{Dest} and key ID's I_i^{Dest} generated as a function of the destination region serviced by the distribution center

92 In response to receiving a mail piece, determine the mail piece's destination region

94 If the distribution center is not within the destination region, transfer the mail piece to the distribution center within the destination region

96 If the distribution center is within the destination region, begin verifying the postage indicia by reading the digital signature and the key ID from the indicia

98 Use the key ID read from the indicia to retrieve the corresponding verification key from the table of all verification keys

100 Use the retrieved verification key to compute a digital signature for the indicia, and compare the computed digital signature with the digital signature from the postage indicia to verify the indicia

Verifying Postage Indicia

FIG. 6

DECLARATION AND POWER OF ATTORNEY FOR UTILITY PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name,

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

EVIDENCING AND VERIFYING INDICIA OF VALUE USING SECRET KEY CRYPTOGRAPHY

the specification of which

X is attached hereto.

___ was filed on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and said invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56 (a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119, of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)**Priority Claimed**

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)

I hereby appoint Joseph A. Sawyer, Jr., Reg. No. 30,801; Stephen G. Sullivan, Reg. No. 38,329; Janyce R. Mitchell, Reg. No. 40,095; Michele Liu, Reg. No.: 44,875; Wendell J. Jones, Reg. No. P45,961 and Doretha L. Robinson, Reg. No. 45,048, of **SAWYER LAW GROUP LLP, located at 2465 E. Bayshore Rd., Suite 406, Palo Alto, California 94303, telephone (650) 493-4540**, as my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to **Stephen G. Sullivan**, at telephone number **(650) 493-4540**, and all correspondence to:

**SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, California 94303**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of sole/first inventor:

Martin J. Pagel

Residence Address:

8515 NE 124th Street

Kirkland

City

King

County

Washington

State

98034

Zip

Post Office Address:

SAME

Country of Citizenship:

Germany

6/30/00
Date

Martin J. Pagel
Signature